Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] 1.A method for managing a buffer memory, the buffer memory is applied to a crypto engine, the crypto engine encrypting or decrypting an input data to produce a result through an encryption algorithm or a decryption algorithm, the method for managing the buffer memory comprising:

defining an input/output(IO) writing address in the buffer memory, the input data being written into the buffer memory beginning at the IO writing address;

defining a program reading address in the buffer memory, the crypto engine reading out the input data beginning at the program reading address to process the encryption algorithm or the decryption algorithm;

defining a program writing address in the buffer memory, the result of the crypto engine being written into the buffer memory beginning at the program writing address;

defining an IO reading address in the buffer memory, the crypto engine reading out the result beginning at the IO reading address and outputting the result;

when the IO writing address is different from the program reading address, controlling the crypto engine to

read the input data beginning at the program reading address; and

when the program writing address is different from the IO reading address, controlling the buffer memory to output the result beginning at the IO reading address.

[c2] 2.The method of claim 1 further comprising:

while the input data is written into the buffer memory, changing the IO writing address in accordance with quantity of the input data;

while the crypto engine reads the input data, changing the program reading address in accordance with quantity of the input data;

while the result is written into the buffer memory, changing the program writing address in accordance with quantity of the result; and

while the buffer memory outputs the result, changing the IO reading address in accordance with quantity of the result.

[c3] 3.The method of claim 1 further comprising:

defining a buffer end address in the buffer memory according to a data length request of the crypto engine processing the encryption algorithm or the decryption algorithm, and dividing the buffer memory into anIO buffer area and a data storage area according to the buffer end address;

storing the input data and the result in the IO buffer area; and

storing a cipher key in the data storage area, wherein the crypto engine utilizes the cipher key to process the encryption algorithm or the decryption algorithm.

[c4] 4.The method of claim 1 further comprising:

while quantity of the input data stored between the IO writing address and the program reading address is smaller than a predetermined quantity, the crypto engine being controlled to suspend reading the input data beginning at the program reading address until quantity of the input data stored between the IO writing address and the program reading address is larger than or equal to the predetermined quantity.